

AMENDMENTS TO THE CLAIMS

1. (Cancelled).

2. (Currently Amended) A method as recited in claim 1, A method of storing a digital asset in a data repository coupled to a network, said method comprising:

receiving, at the data repository, a broadcast cryptographic hash descriptor file identifier that identifies the digital asset;

determining whether the broadcast cryptographic hash descriptor file identifier is a cryptographic hash descriptor file identifier known to the data repository;

when the broadcast cryptographic hash descriptor file is not known to the data repository, adding the broadcast cryptographic hash descriptor file identifier to a list of desired broadcast cryptographic hash descriptor file identifiers;

receiving, at the data repository, the digital asset identified by the broadcast cryptographic hash descriptor file identifier;

generating a generated cryptographic hash descriptor file identifier from the received digital asset; and

verifying that the generated cryptographic hash descriptor file identifier for the received digital asset matches the broadcast cryptographic hash descriptor file identifier, wherein adding the broadcast cryptographic hash descriptor file identifier to the list includes:

determining the number of times the broadcast cryptographic hash descriptor file identifier has been received at the data repository; and

determining whether to add the cryptographic hash descriptor file identifier to said list based upon said number of times.

3. (Currently Amended) A method as recited in claim 1, A method of storing a digital asset in a data repository coupled to a network, said method comprising:

receiving, at the data repository, a broadcast cryptographic hash descriptor file identifier that identifies the digital asset;

determining whether the broadcast cryptographic hash descriptor file identifier is a cryptographic hash descriptor file identifier known to the data repository;

when the broadcast cryptographic hash descriptor file is not known to the data repository, adding the broadcast cryptographic hash descriptor file identifier to a list of desired broadcast cryptographic hash descriptor file identifiers;

receiving, at the data repository, the digital asset identified by the broadcast cryptographic hash descriptor file identifier;

generating a generated cryptographic hash descriptor file identifier from the received digital asset; and

verifying that the generated cryptographic hash descriptor file identifier for the received digital asset matches the broadcast cryptographic hash descriptor file identifier, wherein receiving the digital asset identified by the transmitted cryptographic hash descriptor file identifier includes:

receiving portions of said asset identified by the transmitted cryptographic hash descriptor file identifier at different times; and

assembling the portions of the asset into the complete asset.

4. (Previously Presented) A method as recited in claim 3, further comprising issuing a broadcast request for the digital asset corresponding to the broadcast cryptographic hash descriptor file identifier, and wherein the method further comprises:

ending the broadcast request for portions of the digital asset that have not been obtained.

5. (Previously Presented) A method as recited in claim 4, further comprising: determining an amount of broadcast traffic on at least a portion of the network; and determining whether to send the broadcast request based on the amount of broadcast traffic on the at least a portion of the network.

6. (Currently Amended) ~~A method as recited in claim 1, further comprising:~~ A method of storing a digital asset in a data repository coupled to a network, said method comprising:

receiving, at the data repository, a broadcast cryptographic hash descriptor file identifier that identifies the digital asset;

determining whether the broadcast cryptographic hash descriptor file identifier is a cryptographic hash descriptor file identifier known to the data repository;

when the broadcast cryptographic hash descriptor file is not known to the data repository, adding the broadcast cryptographic hash descriptor file identifier to a list of desired broadcast cryptographic hash descriptor file identifiers;

receiving, at the data repository, the digital asset identified by the broadcast cryptographic hash descriptor file identifier;

generating a generated cryptographic hash descriptor file identifier from the received digital asset;

verifying that the generated cryptographic hash descriptor file identifier for the received digital asset matches the broadcast cryptographic hash descriptor file identifier; and

quarantining the asset while verifying that the generated cryptographic hash descriptor file identifier matches the broadcast cryptographic hash descriptor file identifier.

7-9. (Canceled)

10. (Currently Amended) A method as recited in claim 1, further comprising: A method of storing a digital asset in a data repository coupled to a network, said method comprising:

receiving, at the data repository, a broadcast cryptographic hash descriptor file identifier that identifies the digital asset;

determining whether the broadcast cryptographic hash descriptor file identifier is a cryptographic hash descriptor file identifier known to the data repository;

when the broadcast cryptographic hash descriptor file is not known to the data repository, adding the broadcast cryptographic hash descriptor file identifier to a list of desired broadcast cryptographic hash descriptor file identifiers;

receiving, at the data repository, the digital asset identified by the broadcast cryptographic hash descriptor file identifier;

generating a generated cryptographic hash descriptor file identifier from the received digital asset;

verifying that the generated cryptographic hash descriptor file identifier for the received digital asset matches the broadcast cryptographic hash descriptor file identifier; and

responding to a request, received over the network from another device, for a digital asset stored in the data repository by broadcasting portions of the stored asset; and

broadcasting the portions of the stored asset before the entire asset is received at the data repository.

11-12. (Canceled)

13. (Previously Presented) A method of deleting a digital asset in a data repository that includes an asset list that identifies the digital asset as being stored in the data repository, the method comprising:

receiving, at the data repository, a broadcast cryptographic hash descriptor file identifier;

adding the broadcast cryptographic hash descriptor file identifier to a list of files to be deleted;

comparing the broadcast cryptographic hash asset identifier to a generated cryptographic hash asset identifier for the digital asset; and

deleting the digital asset from the asset list that identifies the digital asset as being stored in the data repository when the broadcast cryptographic hash asset identifier matches the generated cryptographic hash asset identifier.

14-15. (Canceled)